L-BANK
Staatsbank für Baden-Württemberg

Zertifizierungsstelle (CA) der L-BANK

Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS)

Version 2.0

Inhaltsverzeichnis

1 Einleitung

1.1 Überblick

Dieses Dokument fasst die für die Benutzer und die L-BANK als Zertifizierungsinfrastruktur-Betreiber (Public Key Infrastructure – PKI) verbindlichen Inhalte des Sicherheits- und Zertifizierungskonzepts der L-BANK für den Produktivbetrieb der Zertifizierungsstelle in Form einer Zertifizierungsrichtlinie (Certification Policy – CP) und den Regelungen für den Zertifizierungsbetrieb (Certification Practice Statements – CPS) in einem Dokument zusammen.

Die Gliederung erfolgt nach dem Muster des Standards RFC 3647.

Die von der PKI der L-BANK ausgestellten Zertifikate erfüllen die Voraussetzungen der fortgeschrittenen Signatur nach dem Gesetz über Rahmenbedingungen für elektronische Signaturen (SigG).

1.2 Dokumentname sowie Identifikation

Name:	Zertifizierungsstelle der L-BANK Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS)
Version:	2.0
Datum:	23.05.2014
OID:	1.3.6.1.4.1.22064.300.2.1.5.2.0

Der OID ist wie folgt zusammengesetzt:
{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) l-bank(
22064) pki(300) cps(2) x.509(1) global/classic/basic(5) major-version(2) minorversion(
0)}

1.3 Teilnehmer der Zertifizierungsinfrastruktur (PKI)

1.3.1 Zertifizierungsstellen

Für die PKI der L-BANK wird eine einstufige Zertifizierungsstruktur mit einem selbstsignierten Root-Zertifikat verwendet.
Die Root-CA zertifiziert ausschließlich nachgelagerte fachliche CA's, welche verwendet wird, um Benutzerzertifikate zu erstellen.

1.3.2 Registrierungsstellen

Die Registrierungsstellen sind für die Überprüfung der Identität und Authentizität von Zertifikatsnehmern verantwortlich. Das Registrierungsverfahren ist in Abschnitt 3.2.3. dargestellt.

1.3.3 Zertifikatsinhaber bzw. -nehmer

Zertifikatsinhaber bzw. Zertifikatsnehmer sind nur Beschäftigte der L-BANK mit einer persönlichen E-Mail-Adresse.

1.3.4 Zertifikatsnutzer

Zertifikatsnutzer sind Kommunikationspartner (Personen, Organisationen), die am zertifikatsbasierten Verfahren zur sicheren E-Mail-Kommunikation mit der L-BANK teilnehmen.

1.3.5 Weitere Teilnehmer

Entfällt.

1.4 Anwendungsbereich

1.4.1 Geeignete Zertifikatsnutzung

Die ausgestellten Zertifikate sollten nur zur Sicherung der E-Mail-Kommunikation (Verschlüsselung und Signatur) in Zusammenhang mit Geschäftsangelegenheiten der L-BANK verwendet werden.

1.4.2 Untersagte Zertifikatsnutzung

Die private Verwendung der Zertifikate ist untersagt.
Geschäftspartner dürfen die Zertifikate nicht ohne die Genehmigung der L-BANK-PKI über die in Ziffer 1.4.1 beschriebene Verwendung hinaus in Zusammenhang mit Geschäftsangelegenheiten mit Dritten nutzen.

1.5 Verwaltung der Zertifizierungsrichtlinien

1.5.1 Änderungsmanagement

Das Dokument wird von den Betreibern der L-BANK-PKI gepflegt.

1.5.2 Ansprechpartner

L-Bank
Zertifizierungsstelle
Schlossplatz 10
76131 Karlsruhe
Tel.: +49 721 150 3720
e-Mail: securemail@l-bank.de

1.5.3 Eignungsprüfer für Regelungen für den Zertifizierungsbetrieb (CPS) gemäß Zertifizierungsrichtlinie

Die Richtlinien des Zertifizierungsbetriebes sowie dieses Dokument werden durch den Systemeigner der L-BANK-PKI überprüft.

1.5.4 Veröffentlichung von Regelungen für den Zertifizierungsbetrieb (CPS)

Die Zertifizierungsrichtlinie und die Regelungen für den Zertifizierungsbetrieb werden auf der Homepage der L-BANK veröffentlicht.

1.6 Definitionen und Abkürzungen

Siehe Kapitel 10.

2 Verantwortlichkeit für Verzeichnisse und Veröffentlichungen

2.1 Verzeichnisse

Die L-BANK stellt die Informationen zur PKI auf der Homepage (http://www.l-bank.de) sowie im Intranet (Zugriff nur für Beschäftigte der L-BANK) zur Verfügung.

2.2 Veröffentlichung von Zertifizierungsinformationen

Die L-BANK veröffentlicht folgende Informationen:

- CA-Zertifikate mit Fingerprints,
- Root-CA-Zertifikate mit Fingerprints,
- Sperrlisten,
- Erläuterungen zum Sperrverfahren,
- Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS).

2.3 Aktualisierung der Informationen (Zeitpunkt, Frequenz)

Für die Veröffentlichung von CA-/Root-CA-Zertifikaten, Sperrlisten sowie CP/CPS gelten die folgenden Intervalle:

CA-/Root-CA-Zertifikaten	Unmittelbar nach Erzeugung
Sperrlisten	Nach Sperrungen, sonst turnusmäßig (siehe Abschnitt 4.9.7)
CP/CPS	Nach Erstellung bzw. Aktualisierung

2.4 Zugang zu den Informationsdiensten

Der lesende Zugriff auf die unter den Abschnitten 2.1 und 2.2 aufgeführten Informationen ist nicht eingeschränkt. Der schreibende Zugriff liegt im Verantwortungsbereich der L-BANK-PKI.

3 Identifizierung und Authentifizierung

3.1 Namen

3.1.1 Namensformen

Der Name der ausgestellten Zertifikate (Distinguished Name = DN) richtet sich nach den Vorgaben des Standards X.509. Der DN entspricht grundsätzlich folgendem Schema:

E-Mail	<E-Mail-Adresse>
CN	<Name>
OU	<Organisationseinheit>
O	L-Bank
L	Karlsruhe
ST	Baden-Württemberg
C	DE

3.1.2 Aussagekraft von Name

Der Name des ausgestellten Zertifikates (DN) muss den Zertifikatsinhaber eindeutig identifizieren. Es gelten die folgenden Regelungen:

- Zertifikate für natürliche Personen sind auf den Namen des Zertifikatsinhabers auszustellen.
- Zertifikate für organisations- bzw. funktionsbezogene Personengruppen sowie für organisationsbezogene Mailstellen müssen sich deutlich von Zertifikaten für natürliche Personen unterscheiden.

3.1.3 Anonymität bzw. Pseudonyme der Zertifikatsinhaber

Anonymität oder Pseudonymität in Namen von Zertifikaten ist nicht erlaubt.

3.1.4 Regeln zur Interpretation verschiedener Namensformen

Der DN richtet sich nach den Vorgaben des Standards X.509. Das Attribut Alternativer Antragstellername enthält die E-Mail-Adresse in RFC 822 Kodierung. Bei den Namen der Zertifikate für Personen, Gruppen sowie Mailstellen für Beschäftigte der L-BANK gelten zudem die MS Outlook Namenskonventionen der L-BANK.

3.1.5 Eindeutigkeit von Namen

Die Eindeutigkeit von Namen wird von der L-BANK-PKI gewährleistet. Darüber hinaus wird jedem Zertifikat eine eindeutige Seriennummer zugeordnet, welche eine eindeutige und unveränderliche Zuordnung zum Zertifikatsinhaber ermöglicht.

3.1.6 Anerkennung, Authentifizierung und Funktion von Warenzeichen

Im Rahmen der Beantragung von Zertifikaten für Geschäftspartner dürfen nur solche Marken oder Warenzeichen als Teil des Zertifikatseintrags für die im Antrag anzugebende Firma bzw. Behörde verwendet werden, zu deren Verwendung diese berechtigt sind. Diese Berechtigung wird jedoch bei der Registrierung nicht geprüft.

Die L-BANK-PKI bietet insbesondere keine Prozeduren zur Auflösung von Markenstreitigkeiten an. Diese sind zwischen den daran beteiligten Unternehmen ggf. durch markenrechtliche oder wettbewerbsrechtliche Maßnahmen im Zivilrechtsweg zu lösen. Falls der L-BANK-PKI ein rechtskräftiges Urteil vorgelegt wird, das die Unrechtmäßigkeit der Verwendung einer Marke oder eines Warenzeichens feststellt, wird das Zertifikat gesperrt.

3.2 Identitätsüberprüfung bei Neuantrag

3.2.1 Nachweis des Besitzes des privaten Schlüssels

Die Schlüsselpaare der Zertifizierungsstellen sowie der Zertifikatsinhaber werden ausschließlich durch die L-BANK-PKI generiert.

3.2.2 Authentifizierung einer Organisation

Zertifikate für organisationsbezogene Mailstellen bzw. organisations- oder funktionsbezogene Personengruppen werden immer von natürlichen Personen beantragt, deren Authentifizierung über das mehrstufige Registrierungsverfahren gemäß Ziffer 3.2.3 erfolgt.

3.2.3 Authentifizierung natürlicher Personen

Sämtliche Beschäftigte der L-BANK werden grundsätzlich von der zuständigen Personalstelle registriert.
Die Registrierung zur Nutzung von digitalen Zertifikaten erfolgt mehrstufig im Rahmen eines Antragsworkflows über die genehmigenden Vorgesetzten an die L-BANK-PKI.

3.2.4 Nicht überprüfte Teilnehmerangaben

Es werden nur Angaben zur Authentifikation und Identifikation von Zertifikatsinhabern überprüft. Andere Informationen des Zertifikatsinhabers werden nicht berücksichtigt.

3.2.5 Überprüfung der Berechtigung

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Antragsworkflows, der von der jeweiligen Fachstelle zu genehmigen ist.

3.2.6 Kriterien für Zusammenarbeit

Nicht zutreffend. Es ist keine Cross-Zertifizierung mit anderen Organisationen geplant.

3.3 Identifizierung und Authentifizierung bei einer Zertifikatserneuerung

3.3.1 Routinemäßige Zertifikatserneuerung

Vor Ablauf der Gültigkeit eines Zertifikates wird letzteres automatisch erneuert. Eine Beantragung durch den Zertifikatsinhaber ist nicht erforderlich.

3.3.2 Zertifikatserneuerung nach einer Sperrung

Nach einer Sperrung eines Zertifikates muss ein Neuantrag gestellt werden.

3.4 Identifizierung und Authentifizierung von Sperranträgen

Die Sperrung eines Zertifikates kann vom Zertifikatsinhaber, einem vom Zertifikatsinhaber Beauftragten oder vom Vorgesetzten per Antragsworkflow, telefonisch als auch per Telefax oder schriftlich veranlasst werden.
Die Identität des Antragstellers wird von der L-BANK-PKI dokumentiert. Der Zertifikatsinhaber wird über die Sperrung des Zertifikates unterrichtet.

4 Ablauforganisation

4.1 Zertifikatsantrag

4.1.1 Wer kann ein Zertifikat beantragen

Zertifikate können von den in Abschnitt 1.3.3 benannten Personen beantragt werden.

4.1.2 Verfahren und Verantwortungen

Die Beantragung von Zertifikaten erfolgt im Rahmen eines mehrstufigen Antragsworkflows über den genehmigenden Vorgesetzten an die L-BANK-PKI. Dabei werden folgende Prüfungen vorgenommen:

- Berechtigung des Antragstellers,
- Vollständigkeit und Korrektheit des Antrags,
- Eindeutigkeit des DN,
- Prüfung der Authentizität von Personen.

4.2 Bearbeitung von Zertifikatsanträgen

4.2.1 Durchführung von Identifikation und Authentifizierung

Die Identifikation und Authentifizierung von Zertifikatsinhabern wird wie in Kapitel 3.2 beschrieben durchgeführt.

4.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Trotz Erfüllung der formalen Voraussetzungen besteht kein Anspruch auf Erteilung eines Zertifikats.

4.2.3 Bearbeitungsdauer bei Zertifikatsanträgen

Die Bearbeitungsdauer von Zertifikatsanträgen beträgt grundsätzlich maximal eine Woche.

4.3 Ausstellung von Zertifikaten

4.3.1 Aufgaben der Zertifizierungsstelle

Nach der Bearbeitung des Zertifikatsantrages wird das Schlüsselpaar in der L-BANK-PKI durch die Gateway-Software generiert und das Zertifikat erzeugt.

4.3.2 Benachrichtigung des Antragstellers

Nach Erstellung des Zertifikats wird der Antragsteller über dessen Ausstellung informiert.

4.4 Zertifikatsakzeptanz

4.4.1 Annahme des Zertifikats

Die Annahme des Zertifikates erfolgt mit der Nutzung des Zertifikats.

4.4.2 Veröffentlichung des Zertifikats durch die Zertifizierungsstelle

Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst wird nicht ausgeschlossen.

4.4.3 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.5 Verwendung des Schlüsselpaars und des Zertifikats

4.5.1 Nutzung durch den Zertifikatsinhaber

Die Nutzung des privaten Schlüssels ist ausschließlich dem Zertifikatsinhaber vorbehalten. Der Zertifikatsinhaber hat insbesondere die Aufgaben

- unverzüglich anzuzeigen, falls die Angaben in seinem Zertifikat nicht oder nicht mehr den Tatsachen entsprechen,
- die Beschränkungen hinsichtlich der Verwendung seines privaten Schlüssels einzuhalten (siehe Abschnitt 1.4.1),
- unverzüglich die Sperrung des Zertifikates zu veranlassen, wenn sein privater Schlüssel kompromittiert ist oder das Zertifikat nicht länger benötigt wird (siehe Kapitel 4.9).

4.5.2 Nutzung des Zertifikats durch die Relying Party

Der Zertifikatsnutzer darf das Zertifikat nur für die im Zertifikat ausgewiesenen Verwendungszwecke einsetzen. Darüber hinaus muss er die Gültigkeit des Zertifikates überprüfen.

4.6 Zertifikatserneuerung unter Beibehaltung des alten Schlüssels (Certificate Renewal)

Eine Zertifikatserneuerung auf Basis des bestehenden Schlüsselpaares ist nicht zugelassen. Bei der Zertifikatserneuerung wird immer ein neues Schlüsselpaar generiert. Alle nachfolgenden Punkte des Kapitels 4.6 sind daher nicht zutreffend.

4.6.1 Gründe für eine Zertifikatserneuerung

Entfällt.

4.6.2 Wer kann eine Zertifikatserneuerung beantragen

Entfällt.

4.6.3 Ablauf der Zertifikatserneuerung

Entfällt.

4.6.4 Benachrichtigung des Zertifikatsinhabers nach Zertifikatserneuerung

Entfällt.

4.6.5 Annahme einer Zertifikatserneuerung

Entfällt.

4.6.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Entfällt.

4.6.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Entfällt.

4.7 Zertifikatserneuerung mit Schlüsselwechsel (Re-Keying)

Bei der Zertifikatserneuerung wird immer ein neues Schlüsselpaar generiert. Dabei erfolgt stets eine Datenanpassung (siehe Kapitel 4.8). Alle nachfolgenden Punkte des Kapitels 4.7 sind daher nicht zutreffend.

4.7.1 Gründe für eine Schlüssel- und Zertifikatserneuerung

Entfällt.

4.7.2 Wer kann eine Schlüssel- und Zertifikatserneuerung beantragen

Entfällt.

4.7.3 Ablauf der Schlüssel- und Zertifikatserneuerung

Entfällt.

4.7.4 Benachrichtigung des Zertifikatsinhabers

Entfällt.

4.7.5 Annahme der Schlüssel- und Zertifikatserneuerung

Entfällt.

4.7.6 Veröffentlichung einer Zertifikatserneuerung durch die Zertifizierungsstelle

Entfällt.

4.7.7 Benachrichtigung weiterer Instanzen durch die Zertifizierungsstelle

Entfällt.

4.8 Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung

Im Rahmen der L-BANK-PKI findet eine Zertifikatserneuerung mit einem Wechsel des Schlüsselpaars und einer Anpassung von Zertifikatsinhalten sowie technischen Parametern statt.

4.8.1 Gründe für eine Zertifikatsmodifizierung

Die nachfolgenden Gründe führen zu einer Zertifikatserneuerung mit Schlüsselwechsel und Datenanpassung:

- Routinemäßige Zertifikatserneuerung
  - bei bevorstehendem Ablauf der Gültigkeit des Zertifikates oder
  - bereits erfolgtem Ablauf der Gültigkeit des Zertifikates.
- Zertifikatsbeantragung nach einer Sperrung des bisherigen Zertifikates.
- Die Daten des Zertifikates entsprechen nicht oder nicht mehr den Tatsachen.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr oder eine Erneuerung der Zertifikatsstruktur ist zwingend erforderlich.

4.8.2 Wer kann eine Zertifikatsmodifizierung beantragen

Die Zertifikatserneuerung wird vom Zertifikatsinhaber über einen mehrstufigen Antragsworkflow beantragt.
Falls die Schlüssellänge, die Gültigkeitsdauer oder die Zertifikatsstruktur aus Sicherheitsgründen außerplanmäßig die Erneuerung von Zertifikaten erforderlich machen sollte, wird die Zertifikatserneuerung von der L-BANK-PKI ohne ein vorheriges Antragsverfahren durchgeführt. Die Zertifikatsinhaber werden über die erfolgte außerplanmäßige Zertifikatserneuerung informiert.

4.8.3 Ablauf der Zertifikatsmodifizierung

Der Prozess der Zertifikatserneuerung entspricht dem Verfahren der erstmaligen Antragstellung. Das Schlüsselpaar in der L-BANK-PKI wird durch die Gateway-Software generiert und das Zertifikat erzeugt.

4.8.4 Benachrichtigung des Zertifikatsinhabers

Nach Erstellung des Zertifikats wird der Zertifikatsinhaber über dessen Ausstellung informiert.

4.8.5 Annahme der Zertifikatsmodifizierung

Die Annahme des Zertifikates erfolgt mit der Nutzung des Zertifikates.

4.8.6 Veröffentlichung einer Zertifikatsmodifizierung durch die Zertifizierungsstelle

Eine Veröffentlichung der Zertifikate in einem Verzeichnisdienst wird nicht ausgeschlossen.

4.8.7 Benachrichtigung weiterer Instanzen über die Zertifikatserneuerung

Eine Benachrichtigung weiterer Instanzen ist nicht erforderlich.

4.9 Sperrung und Suspendierung von Zertifikaten

4.9.1 Gründe für Widerruf / Sperrung

Ein Zertifikat muss gesperrt werden, wenn mindestens einer der folgenden Gründe eintritt:

- Die im Zertifikat enthaltenen Angaben sind nicht oder nicht mehr gültig.
- Der private Schlüssel wurde kompromittiert.
- Der Zertifikatsinhaber ist nicht mehr berechtigt, das Zertifikat zu nutzen.
- Der Zertifikatsinhaber benötigt das Zertifikat nicht mehr.
- Der Zertifikatsinhaber hält diese Zertifizierungsrichtlinie (CP) und die Regelungen für den Zertifizierungsbetrieb (CPS) nicht ein.
- Die L-BANK-PKI stellt ihren Zertifizierungsbetrieb ein. In diesem Fall werden sämtliche von der L-BANK-PKI ausgestellten Zertifikate gesperrt.
- Der private Schlüssel der ausstellenden oder einer übergeordneten Root-CA wird kompromittiert. In diesem Fall werden sämtliche von diesen CA's ausgestellte Zertifikate gesperrt.
- Die Algorithmen, die Schlüssellänge oder die Gültigkeitsdauer des Zertifikates bieten keine ausreichende Sicherheit mehr. Die L-BANK-PKI behält sich vor, die betreffenden Zertifikate zu sperren.

4.9.2 Wer kann Widerruf / Sperrung beantragen

Die Sperrung eines Zertifikates kann vom Zertifikatsinhaber, einem vom Zertifikatsinhaber Beauftragten oder vom Vorgesetzten beauftragt werden.
Der Zertifikatsinhaber kann die Sperrung seines eigenen Zertifikates jederzeit beantragen, auch wenn keiner der in Ziffer 4.9.1 genannten Gründe vorliegt.

4.9.3 Ablauf von Widerruf / Sperrung

Die Sperrung eines Zertifikates kann

- per Antragsworkflow,
- telefonisch,
- per Telefax oder
- schriftlich

erfolgen.

Die L-BANK-PKI führt die Sperrung des Zertifikates an der entsprechenden CA durch und veröffentlicht die entsprechende Sperrliste. Der Zertifikatsinhaber wird über die Sperrung des Zertifikates unterrichtet.

4.9.4 Fristen für den Zertifikatsinhaber

Die Zertifikatsinhaber sind bei bekannt werden eines Sperrgrundes verpflichtet, unverzüglich die Sperrung des Zertifikates zu veranlassen.

4.9.5 Bearbeitungsfristen für die Zertifizierungsstelle

Die Sperrung des Zertifikates wird von der L-BANK-PKI unverzüglich nach Zugang des Sperrantrages durchgeführt.

4.9.6 Anforderung zu Sperrprüfungen durch den Zertifikatsnutzer

Sperrinformationen werden mittels Sperrlisten veröffentlicht. Zur Prüfung der Gültigkeit von Zertifikaten muss der Zertifikatsnutzer jeweils die aktuell veröffentlichte Sperrliste verwenden.

4.9.7 Häufigkeit der Sperrlistenveröffentlichung

CA-Sperrlisten und Root-CA-Sperrlisten werden immer bei Abruf am CDP (CRL Distribution Point) adhoc erstellt.

4.9.8 Maximale Latenzzeit für Sperrlisten

Die Veröffentlichung von Sperrlisten wird unmittelbar nach deren Erzeugung veranlasst.

4.9.9 Verfügbarkeit von Online-Statusabfragen (OCSP)

Entfällt. Online Sperrungen und Statusprüfungen stehen z. Z. nicht zur Verfügung.

4.9.10 Anforderungen an Online-Statusabfragen (OCSP)

Entfällt.

4.9.11 Andere verfügbare Formen der Widerrufsbekanntmachung

Entfällt. Andere Formen zur Anzeige von Sperrinformationen werden nicht angeboten.

4.9.12 Anforderungen bei Kompromittierung von privaten Schlüsseln

Bei der Kompromittierung des privaten Schlüssels eines Zertifikatsinhabers ist das zugehörige Zertifikat unverzüglich zu sperren. Bei der Kompromittierung des privaten Schlüssels einer CA werden neben dem CA-Zertifikat auch alle von ihr ausgestellten Zertifikate gesperrt.

4.9.13 Gründe für eine Suspendierung

Eine temporäre Sperrung bzw. eine Suspendierung von Zertifikaten ist nicht erlaubt. Einmal gesperrte Zertifikate können nicht reaktiviert werden.

4.9.14 Wer kann Suspendierung beantragen

Entfällt.

4.9.15 Ablauf einer Suspendierung

Entfällt.

4.9.16 Maximale Sperrdauer bei Suspendierung

Entfällt.

4.10 Dienst zur Statusabfrage von Zertifikaten (OCSP)

Die L-BANK-PKI unterhält keinen Dienst zur Statusabfrage von Zertifikaten. Die Bereitstellung von Sperrlisten ist in Kapitel 2 geregelt.

4.10.1 Betriebsbedingte Eigenschaften

Entfällt.

4.10.2 Verfügbarkeit des Dienstes

Entfällt.

4.10.3 Weitere Merkmale

Entfällt.

4.11 Beendigung der Zertifikatsnutzung durch den Zertifikatsinhaber

Eine Beendigung der Zertifikatsnutzung durch den Zertifikatsinhaber erfolgt entweder durch die Sperrung des Zertifikates oder indem nach Ablauf der Gültigkeit kein neues Zertifikat beantragt wird.

4.12 Schlüsselhinterlegung und –wiederherstellung

Eine Schlüsselhinterlegung und –wiederherstellung durch die L-BANK-PKI wird nicht angeboten.

4.12.1 Richtlinien und Praktiken zur Schlüsselhinterlegung und –wiederherstellung

Entfällt.

4.12.2 Richtlinien und Praktiken zum Schutz und Wiederherstellung von Sitzungsschlüsseln

Entfällt.

5 Infrastrukturelle, organisatorische und personelle Sicherheitsmaßnahmen

5.1 Infrastrukturelle Sicherheitsmaßnahmen

5.1.1 Einsatzort und Bauweise

Die L-BANK-PKI wird innerhalb eines zugangsgesicherten Bereiches mit einem weiteren separaten Sicherheitsbereich betrieben. Sie unterhält darüber hinaus verschiedene Sicherheitsanlagen zur Hinterlegung von Produktiv- und Backup-Systemen und –Medien.
Der Sicherheitsbereich sowie die Sicherheitsanlagen sind an die zentrale Alarmleitstelle des Gebäudes angebunden. Zudem ist der Sicherheitsbereich an ein lokales optisches und akustisches Alarmsystem angeschlossen.

5.1.2 Räumlicher Zugang

Der räumliche Zugang erfolgt über ein mehrstufiges Zugangskontrollsystem. Zu dem Sicherheitsbereich der L-BANK-PKI ist ausschließlich das dort produktiv tätige PKI-Betriebspersonal zutrittsberechtigt. Es wird ein ausweisbezogenes Login mit biometrischer Bestätigung durchgeführt.

5.1.3 Stromversorgung und Klimaanlagen

Die Installation zur Stromversorgung entspricht den erforderlichen Normen. Eine Notstromversorgung über Dieselgeneratoren ist vorhanden. Eine Klimatisierung des Sicherheitsbereiches ist vorhanden.

5.1.4 Gefährdung durch Wasser

Die Räume verfügen über einen angemessenen Schutz vor Wasserschäden.

5.1.5 Brandschutz

Die Richtlinien für den Brandschutz werden eingehalten. Die Räume sind über Rauchmelder an die Brandmeldeanlage angeschlossen und enthalten eine automatische Löschanlage. Handfeuerlöscher sind in angemessener Anzahl vorhanden.

5.1.6 Aufbewahrung von Datenträgern

Sämtliche Datenträger mit Software sowie tagesaktuellen Sicherungen werden in mehrfachen Ausfertigungen als Original- und Backup-Versionen vorgehalten und in unterschiedlichen Gebäude (am Hauptsitz Karlsruhe und in der Niederlassung Stuttgart) sicher aufbewahrt. Darüber hinaus werden der Gesamtbestand außer Kraft gesetzter Software sowie alte Datensicherungen in einem Archiv hinterlegt.
Sämtliche Datenträger werden mehrstufig in anwendungsbezogenen Stahlkassetten, die sich in Tresorschränken befinden, sicher hinterlegt.

5.1.7 Entsorgung von Datenträgern

Elektronische Datenträger und Papierdatenträger werden vor Ort in abschließbaren Stahlbehältern gesammelt und an einem Dienstleister zur sachgerechten Entsorgung weitergeleitet.

5.1.8 Externe Datensicherung

Eine externe Sicherung von Daten außerhalb der L-BANK-PKI bei anderen Dienstleistern findet nicht statt.

5.2 Organisatorische Sicherheitsmaßnahmen

5.2.1 Rollenkonzept

Es wird im Rahmen eines Rollenkonzeptes sichergestellt, dass einzelne Personen nicht unbemerkt Veränderungen an sicherheitskritischen Komponenten der L-BANK-PKI vornehmen können und Zertifikate oder private Schlüssel einsehen, generieren oder manipulieren können. Die Namen der am Prozess der Generierung sowie Auslieferung von Schlüsseln und Zertifikaten beteiligten Personen werden protokolliert.

5.2.2 Anzahl involvierter Personen pro Aufgabe

Die L-BANK-PKI setzt im Produktionsbetrieb für den Umgang mit hochsicherheitskritischen Zugangsmedien und kryptographischen Schlüsselmaterialien und Zertifikaten ein strenges durchgängiges Vier-Augen-Prinzip ein.
Das Konzept sieht vor, dass die Hinterlegung, der Zugriff und der Einsatz der hochsicheren Zugangsmedien stets vom PKI-Betriebspersonal im Vier-Augen-Prinzip wahrgenommen werden. Darüber hinaus wird der gesamte Prozess der Generierung von kryptographischem Schlüsselmaterial und Zertifikaten bis zur Weitergabe im Vier-Augen-Prinzip durchgeführt. Das durchgängige Vier-Augen-Prinzip setzt die Dokumentation der Rollenverteilung der am Generierungsprozess beteiligten Personen in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen voraus (siehe Ziffer 5.2.1).

5.2.3 Identifizierung und Authentifizierung jeder Rolle

Das Rollenkonzept wird durch technische und organisatorische Maßnahmen umgesetzt. Die Identifizierung und Authentifizierung der Rollen erfolgt

- beim Zutritt zu Sicherheitsbereichen und Tresoren bzw.
- beim Zugriff auf Wertschränke oder sicherheitskritische Systeme und Anwendungen

mit Hilfe von SmartCards, Benutzerkennungen und Passwörtern.
Die Rollenverteilung wird in verschiedenen zu erstellenden sowie systembedingt erzeugten Protokollen dokumentiert (siehe Ziffer 5.2.1).

5.2.4 Rollen, die eine Aufgabentrennung erfordern

Das Rollenkonzept stellt die Trennung von bestimmten Rollen und Aufgaben sicher, um zu verhindern, dass eine Person allein einen Schlüssel erzeugen oder ein Zertifikat ausstellen und weitergeben kann.

5.3 Personelle Sicherheitsmaßnahmen

5.3.1 Anforderungen an Mitarbeiter

Die L-BANK-PKI setzt im Betrieb erfahrenes Personal ein, das über die erforderlichen IT-Kenntnisse und spezifischen Kenntnisse des CA-Betriebs verfügt.

5.3.2 Sicherheitsüberprüfung der Mitarbeiter

Von allen Mitarbeitern der L-BANK-PKI liegt ein polizeiliches Führungszeugnis vor.

5.3.3 Anforderungen an Schulungen

Das mit dem Betrieb der L-BANK-PKI betraute Personal wird regelmäßig und anlassbezogen geschult. Es ist hinsichtlich der Sicherheitsrelevanz seiner Arbeit sensibilisiert.

5.3.4 Häufigkeit und Anforderungen an Fortbildungen

Schulungen und Fortbildungen werden insbesondere bei der Einführung neuer Richtlinien, IT-Systeme und IT-Verfahren durchgeführt.

5.3.5 Häufigkeit und Ablauf von Arbeitsplatzwechseln

Das PKI-Betriebspersonal wird in allen Bereichen des CA-Betriebes eingesetzt.

5.3.6 Sanktionen für unerlaubte Handlungen

Unerlaubte Handlungen, die die Sicherheit der L-BANK-PKI gefährden oder gegen Datenschutzbestimmungen verstoßen, werden über die Personalstellen disziplinarisch geahndet bzw. strafrechtlich verfolgt.

5.3.7 Anforderungen an unabhängige, selbstständige Zulieferer

Entfällt.

5.3.8 Dokumentation für Mitarbeiter

Dem Personal der L-BANK-PKI stehen zum ordnungsgemäßen Betrieb der PKI folgende Dokumente zur Verfügung:

- Zertifizierungsrichtlinie (CP) und Regelungen für den Zertifizierungsbetrieb (CPS),
- Betriebshandbücher,
- Benutzeranleitungen,
- Dienstvorschriften und -anweisungen.

5.4 Überwachung / Protokollierung

5.4.1 Überwachte Ereignisse

Die nachfolgenden Ereignisse werden protokolliert und dokumentiert:

- Systeminitialisierung,
- Zertifizierungsanträge,
- Registrierung der Benutzer,
- Schlüsselerzeugung für CA, Root-CA, Benutzer,
- Zertifikatserstellung für CA, Root-CA, Benutzer,
- Datensicherungen für CA, Root-CA
- Zertifikatsveröffentlichung CA, Root-CA
- Auslieferung des privaten Schlüssels und des Zertifikates,
- Sperranträge,
- Sperrung eines Zertifikates,
- Erstellung einer Sperrliste,
- Veröffentlichung einer Sperrliste.

Darüber hinaus werden Störfälle und besondere Betriebssituationen erfasst. ???

5.4.2 Häufigkeit der Protokollanalyse

Die Ordnungsmäßigkeit des Zertifizierungsbetriebes wird im Rahmen der risikoorientierten Prüfungen des Bereiches Revision der L-BANK vorgenommen. Bei Verdacht auf Unregelmäßigkeiten wird eine umgehende Prüfung veranlasst.

5.4.3 Aufbewahrungsfrist für Protokolldaten

Die Aufbewahrungszeiten orientieren sich an gesetzlichen Fristen, den Grundsätzen der Revisionssicherheit sowie der weiteren internen Regelungen.

5.4.4 Schutz von Protokolldaten

Die Protokolle werden gegen Zugriff, Manipulation und Vernichtung geschützt.

5.4.5 Backup der Protokolldaten

Die Protokolldaten werden zusammen mit anderen relevanten Daten einem regelmäßigen Backup unterzogen. Protokolle auf Papier werden in verschließbaren Schränken verwahrt.

5.4.6 Überwachungssystem (intern oder extern)

Entfällt.

5.4.7 Benachrichtigung bei schwerwiegenden Ereignissen

Bei Eintreten von sicherheitskritischen Ereignissen unterrichtet die L-BANK-PKI die zuständige Stelle für IT-Sicherheitsvorfälle und den Systemeigner.

5.4.8 Schwachstellenanalyse

Eine Schwachstellenanalyse kann im Bedarfsfall jederzeit durchgeführt werden.

5.5 Archivierung

5.5.1 Archivierte Daten

Sämtliche Daten, die für den Zertifizierungsprozess relevant sind (siehe Abschnitt 5.4.1) werden archiviert.

5.5.2 Aufbewahrungsfrist für archivierte Daten

Die Aufbewahrungsfristen sind in Abschnitt 5.4.3 geregelt.

5.5.3 Schutz der Archive

Die Archive werden gegen Zugriff, Manipulation und Vernichtung geschützt.

5.5.4 Backup der Archive (Datensicherungskonzept)

Datensicherungen werden arbeitstäglich nach der Durchführung von

- Schlüsselausgaben,
- Sperrungen von Zertifikaten sowie
- der Erstellung von Sperrlisten

durchgeführt. Sie werden als Original- und Backupdatensicherungen vorgenommen und sicher in unterschiedlichen Gebäudebrandabschnitten hinterlegt.

5.5.5 Anforderungen an Zeitstempel

Entfällt.

5.5.6 Archivierungssystem (intern oder extern)

Die Archivierung wird bei der L-BANK-PKI vorgenommen.

5.5.7 Prozeduren für Abruf und Überprüfung archivierter Daten

Ein standardisiertes Verfahren zum Abruf und Überprüfen archivierter Daten wird nicht angeboten.

5.6 Schlüsselwechsel der Zertifizierungsstelle

Ein Schlüsselwechsel der Zertifizierungsstelle erfolgt spätestens dann, wenn die Gültigkeit der auszustellenden Benutzerzertifikate die Restlaufzeit der CA übersteigen würde.

5.7 Kompromittierung und Wiederherstellung

5.7.1 Vorgehen bei Sicherheitsvorfällen und Kompromittierung

Das Verfahren zur Behandlung von Sicherheitsvorfällen und Kompromittierungen von privaten Schlüsseln wird von der zuständigen Stelle für IT-Sicherheitsvorfälle festgelegt.

5.7.2 Betriebsmittel, Software und/oder Daten sind korrumpiert

Werden innerhalb der Zertifizierungsstelle fehlerhafte oder manipulierte Rechner, Software und/oder Daten festgestellt, die Auswirkungen auf die Prozesse der Zertifizierungsstelle haben, wird der Betrieb des entsprechenden Systems unverzüglich eingestellt.

Das System wird unter Verwendung der Software sowie der Datensicherungen neu aufgesetzt und nach Überprüfung in einem sicheren Zustand in Betrieb genommen. Das fehlerhafte oder modifizierte System wird analysiert. Bei Verdacht einer vorsätzlichen Handlung werden gegebenenfalls rechtliche Schritte eingeleitet.

Falls Zertifikate mit fehlerhaften Angaben generiert wurden, wird der Zertifikatsinhaber unverzüglich informiert und das Zertifikat von der Zertifizierungsstelle gesperrt.

5.7.3 Kompromittierung des privaten Schlüssels

Bei Kompromittierung des privaten Schlüssels einer Zertifizierungsstelle ist das jeweilige Zertifikat sofort zu sperren. Gleichzeitig sind alle von dieser Zertifizierungsstelle ausgestellten Zertifikate der Zertifikatsinhaber zu sperren. Alle betroffenen Zertifikatsinhaber werden umgehend benachrichtigt.

Die betreffende CA wird als neue Zertifizierungsstelle mit einem neuen Schlüsselpaar aufgesetzt. Das Zertifikat der neuen Zertifizierungsstelle ist zu veröffentlichen und die zuvor gesperrten Zertifikate der Zertifikatsinhaber sind neu auszustellen.

5.7.4 Wiederaufnahme des Betriebs nach einem Notfall

Eine Wiederaufnahme des Zertifizierungsbetriebes nach einer Katastrophe ist Bestandteil der Notfallplanung und kann innerhalb kurzer Zeit erfolgen, sofern die Sicherheit des Betriebes der L-BANK-PKI gegeben ist.

5.8 Einstellung des Betriebs

Im Fall der Einstellung des Betriebes der L-BANK-PKI werden die nachfolgenden Maßnahmen ergriffen:

- Information aller Zertifikatsinhaber sowie vertrauenden Parteien mit einer Vorlauffrist von mindestens drei Monaten.
- Sperrung aller Benutzerzertifikate sowie der Zertifikate der Zertifizierungsstellen.
- Vernichtung der privaten Schlüssel der Zertifizierungsstellen.
- Veröffentlichung der entsprechenden CA- und Root-CA-Sperrlisten.

6 Technische Sicherheitsmaßnahmen

6.1 Schlüsselerzeugung und Installation

6.1.1 Schlüsselerzeugung

Die Schlüsselerzeugung findet innerhalb des Totemo-Gateways automatisch nach Zuweisung der Berechtigung an den Antragsteller statt.

6.1.2 Übermittlung privater Schlüssels an Zertifikatsinhaber

Alle privaten Schlüssel werden im Totemo-Gateway verwaltet. Eine Übermittlung an Zertifikatsinhaber findet nicht statt.

6.1.3 Übermittlung öffentlicher Schlüssels an Zertifikatsaussteller

Nicht zutreffend. Eine Schlüsselerzeugung durch den Zertifikatsinhaber ist nicht vorgesehen.

6.1.4 Übermittlung öffentlicher CA Schlüssels an Zertifikatsprüfer (Relying Parties)

Mit Bereitstellung des Schlüsselpaares wird ebenfalls die Zertifikatskette zur Verfügung gestellt. Die öffentlichen Schlüssel der CA können zudem über den Zertifikatsdienst gemäß Kapitel 2 abgerufen werden.

6.1.5 Schlüssellängen

Es werden nur Kombinationen aus Schlüsselalgorithmus und -länge verwendet, die laut Bundesnetzagentur als sicher eingestuft werden können.
Die CA-Schlüssel der CA/Root-CA haben eine Mindestlänge von 4096 bit. Für Zertifikatsinhaber werden Schlüssel mit einer Länge von mindestens 2048 bit generiert.

6.1.6 Erzeugung der Public Key Parameter und Qualitätssicherung

Es wird folgender Verschlüsselungsalgorithmus verwendet:

- RSA mit OID 1.2.840.113549.1.1.1
- SHA1 RSA 1.2.840.113549.1.1.5

6.1.7 Schlüsselverwendungszwecke (X.509v3 Key Usage)

Private CA-Schlüssel werden ausschließlich zum Signieren von Zertifikaten und Sperrlisten genutzt.

6.2 Schutz des privaten Schlüssels und Einsatz kryptographischer Module

Die privaten Schlüssel werden kryptographisch gesichert hinterlegt.

6.2.1 Standard kryptographischer Module

Die kryptographischen Schutzmechanismen orientieren sich an internationalen Standards.
Gateway Lösung Zugriffsschutz ???

6.2.2 Aufteilung privater Schlüssel auf mehrere Personen (n-aus-m)

Die privaten Schlüssel einer CA sind durch ein Vier-Augen-Prinzip geschützt.

6.2.3 Hinterlegung privater Schlüssel (Key Escrow)

Der private CA-Schlüssel der L-BANK-PKI wird nicht bei Dritten hinterlegt.

6.2.4 Backup privater Schlüssel

Es liegt ein kryptographisch gesichertes Backup der privaten CA-Schlüssel vor. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem. Der Zugriff erfolgt im Vier-Augen-Prinzip.
Für private Schlüssel der Zertifikatsinhaber wird ein Backup über unsere Datenbanksicherung durchgeführt.

6.2.5 Archivierung privater Schlüssel

Nach Ablauf bzw. Sperrung der CA werden die privaten Schlüssel der CA noch 10 Jahre lang aufbewahrt. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem.

6.2.6 Transfer privater Schlüssel in oder aus einem kryptographischen Modul

Ein Transfer privater CA-Schlüssel erfolgt nur zu Backup- oder Wiederherstellungszwecken. Es gelten die identischen Schutzmaßnahmen wie für das Produktivsystem.

6.2.7 Speicherung privater Schlüssel in einem kryptographischen Modul

Das Schlüsselpaar der Zertifizierungsstelle wird in einem kryptographisch gesicherten Speicher hinterlegt.

6.2.8 Aktivierung privater Schlüssel

Die Aktivierung des privaten CA-Schlüssels ist nur im Vier-Augen-Prinzip möglich.
Die Aktivierung des privaten Schlüssels der Zertifikatsinhaber erfolgt mit der erstmaligen Nutzung des Zertifikates.

6.2.9 Deaktivierung privater Schlüssel

Die Deaktivierung des privaten Schlüssels einer CA erfolgt automatisch nach Beendigung des Zertifizierungsprozesses.

6.2.10 Vernichtung privater Schlüssel

Nach Ablauf der Gültigkeit bzw. nach Sperrung des privaten CA-Schlüssels werden diese nach einer Aufbewahrungsfrist von 10 Jahren gelöscht. Die Speichermedien werden zerstört bzw. sicher gelöscht.

6.2.11 Güte kryptographischer Module

Siehe Abschnitt 6.2.1.

6.3 Weitere Aspekte des Schlüsselmanagements

6.3.1 Archivierung öffentlicher Schlüssel

Sämtliche von der L-BANK-PKI erstellten öffentlichen Schlüssel werden in der Datenbank der Zertifizierungsstelle archiviert.

6.3.2 Gültigkeit von Zertifikaten und Schlüsselpaaren

Die von der L-BANK-PKI ausgestellten Zertifikate haben folgende Gültigkeitsdauer:

- Root-CA Zertifikate: 20 Jahre,
- Benutzerzertifikate: 2 Jahre.

6.4 Aktivierungsdaten

Im Rahmen der L-BANK-PKI ist der Zugriff auf die privaten Schlüssel der Zertifizierungsstelle sowie der Benutzer kryptographisch und durch ein Vier-Augen-Prinzip geschützt.

6.4.1 Erzeugung und Installation der Aktivierungsdaten

Die Aktivierungsdaten werden bei der Generierung der Zertifikate erstellt. Für Passwörter werden nicht triviale Kombinationen aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen verwendet. Die Länge muss mindestens 15 Zeichen betragen.

6.4.2 Schutz der Aktivierungsdaten

Die Aktivierungsdaten sind geeignet vor Verlust, Diebstahl, Veränderung, nicht autorisiertem Offenlegen sowie nicht autorisierter Verwendung geschützt.

6.4.3 Weitere Aspekte

Entfällt.

6.5 Sicherheitsmaßnahmen für Computer

6.5.1 Spezifische Anforderungen an technische Sicherheitsmaßnahmen

Alle IT-Systeme der L-BANK-PKI müssen über Betriebssysteme mit aktuellen Sicherheitspatches und Virenscanner verfügen. Die L-BANK-PKI wird als Teil der E-Mail- Gateway-Lösung betrieben. Die Zugriffskontrolle ist als Sicherheitsmaßnahme umgesetzt.

6.5.2 Güte der Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen entsprechen dem aktuellen Stand der Technik. Eine Bedrohungsanalyse wurde durchgeführt sowie ein Sicherheitskonzept erstellt.

6.6 Technische Maßnahmen im Lebenszyklus

6.6.1 Maßnahmen der Systementwicklung

Der Systemeigner ist in die Systementwicklung der L-BANK-PKI Komponenten eingebunden. Die verwendete Software hält allgemein bekannten Bedrohungsszenarien stand.

6.6.2 Maßnahmen im Sicherheitsmanagement

Die Betriebsstelle der L-BANK-PKI wurde im erhöhten Sicherheitsbedarf der Anwendung unterwiesen.
Es wird sichergestellt, dass Systementwickler keinen Zugang zur Betriebsumgebung sowie zu Betriebsdaten haben.

6.6.3 Lebenszyklus der Sicherheitsmaßnahmen

Ausgetauschte IT-Systeme oder –Komponenten werden derart außer Betrieb genommen, dass ein Funktions- und Datenmissbrauch ausgeschlossen wird. Veränderungen an den IT-Systemen oder –Komponenten werden zudem papiergebunden protokolliert.

6.7 Sicherheitsmaßnahmen für das Netzwerk

Die Gateway-Lösung und damit auch die PKI ist durch ein mehrstufiges Firewall-System geschützt.

6.8 Zeitstempel

Ein Zeitstempeldienst wird nicht angeboten.

7 Profile von Zertifikaten, Sperrlisten und Online-Statusabfragen

7.1 Zertifikatsprofil

7.1.1 Versionsnummer

Von der L-BANK-PKI werden Zertifikate entsprechend des Standards X509v3 ausgestellt.

7.1.2 Zertifikatserweiterungen

CA-Zertifikate enthalten folgende Erweiterungen:

Basic Constraints	critical, CA:TRUE,
Authority Key Identifier	160-bit SHA-1 Hash des Ausstellerschlüssels
Subject Key Identifier	160-bit SHA-1 Hash des Ausstellerschlüssels

Benutzerzertifikate enthalten folgende unkritische Erweiterungen:

Key Usage	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, E-mail Protection
Basic Constraints	critical, CA:FALSE
Subject Alt Name	Emailadresse
Issuer Alt Name	Emailadresse
Netscape Zertifikatstyp	SMIME
Netscape Kommentar	Totemo TrustMail - Securing Your Data in Motion
Authority Key Identifier	160-bit SHA-1 Hash des Ausstellerschlüssels
Subject Key Identifier	160-bit SHA-1 Hash des Ausstellerschlüssels
CRL Distribution Points	Full Name: URI:http://securemail.l-bank.de/CRL/ ServiceHandler?service=createCRL&caId=65_1

Seriennummern werden von der L-BANK-PKI nicht zweimal vergeben und sind damit eindeutig.

7.1.3 Algorithmus Bezeichner (OID)

In den von der L-BANK-PKI ausgestellten Zertifikaten wird der Algorithmus RSA verwendet (2.048 Bit).

7.1.4 Namensformen

Die von der Root-CA ausgestellten CA-Zertifikate enthalten den kompletten DN (Distinguished Name) im Subject Name und im Issuer Name Feld.

Der Name der ausgestellten CA-Zertifikate richtet sich nach den Vorgaben des Standards X.509 und entspricht folgendem Schema:

EMAIL:	keine
CN:	L-Bank Root

OU: IS
O: L-BANK
L: Karlsruhe
ST: Baden-Württemberg
C: DE

Die Namen der ausgestellten Benutzerzertifikate richten sich nach den Vorgaben des Standards X.509 und entsprechen folgenden Schemen:

EMAIL: E-Mail-Adresse
CN: Vorname Nachname
OU: IS
O: L-BANK
L: Karlsruhe
ST: Baden-Württemberg
C: DE

7.1.5 Namensbeschränkungen

Siehe Kapitel 3.1.

7.1.6 Bezeichner für Zertifizierungsrichtlinien (OID)

Die L-BANK-PKI Zertifizierungsrichtlinien-OID lautet: 1.3.6.1.4.1.22064.300.2.1.5.0.3.

7.1.7 Nutzung von Erweiterungen zur Richtlinienbeschränkungen (PolicyConstraints)

Entfällt.

7.1.8 Syntax und Semantik von Policy Qualifiern

Entfällt.

7.1.9 Verarbeitung von kritischen Erweiterungen für Zertifizierungsrichtlinien (certificatePolicies)

Entfällt.

7.2 Sperrlistenprofil

7.2.1 Versionsnummer

Die L-BANK-PKI stellt Sperrlisten gemäß der Norm X.509 in der Version 1 aus.

7.2.2 Sperrlisten- und Sperrlisteneintragserweiterungen

In den Benutzerzertifikaten ist ein Sperrlistenverteilpunkt (CRLDP) enthalten.

7.3 OCSP Profil

Entfällt. OSCP wird durch die L-BANK-PKI nicht unterstützt.

7.3.1 Versionsnummer

Entfällt.

7.3.2 OCSP Erweiterungen

Entfällt.

8 Konformitätsprüfung (Compliance Audit, Assesments)

Die Arbeitsprozesse der Zertifizierungsstelle sowie der an der Registrierung beteiligten Stellen werden regelmäßig bzw. anlassbezogen überprüft.
Die Audits des technischen Aufbaus der PKI und der operativen Abläufe werden in regelmäßigen Abständen durch die interne Revision nach den in der L-BANK für solche Vorgänge festgelegten Regeln durchgeführt. Die Ergebnisse der Audits werden nicht veröffentlicht.

8.1 Frequenz und Umstände der Überprüfung

Grundsätzlich werden interne Audits und Prüfungen in regelmäßigen Abständen vorgenommen.

8.2 Identität und Qualifikation des Überprüfers

Die internen Prüfungen werden durch den Bereich Revision, durch den Systemeigner sowie die Leitung der L-BANK-PKI vorgenommen. Die Prüfer verfügen über das Know-how sowie die notwendigen Kenntnisse auf dem Gebiet Public Key Infrastructure (PKI), um die Prüfungen vornehmen zu können.

8.3 Verhältnis von Prüfer zu Überprüftem

Der Prüfer darf nicht in den Produktionsprozess der L-BANK-PKI eingebunden sein. Eine Selbstüberprüfung ist nicht erlaubt.

8.4 Überprüfte Bereiche

Es können alle für die PKI relevanten Bereiche überprüft werden. Die Prüfungsinhalte obliegen dem Prüfer.

8.5 Mängelbeseitigung

Festgestellte Mängel müssen in Abstimmung zwischen Zertifizierungsstelle und Prüfer zeitnah beseitigt werden. Der Prüfer wird über die Beseitigung der Mängel informiert.

8.6 Veröffentlichung der Ergebnisse

Eine Veröffentlichung der Prüfungsergebnisse ist nicht vorgesehen.

9 Weitere geschäftliche und rechtliche Regelungen

9.1 Gebühren

9.1.1 Gebühren für Zertifikatserstellung oder –erneuerung

Es werden keine Gebühren erhoben.

9.1.2 Gebühren für Zugriff auf Zertifikate

Es werden keine Gebühren erhoben.

9.1.3 Gebühren für Sperrung oder Statusabfragen

Es werden keine Gebühren erhoben.

9.1.4 Andere Gebühren

Es werden keine Gebühren erhoben.

9.1.5 Gebührenerstattung

Es werden keine Gebühren erhoben.

9.2 Finanzielle Verantwortung

Eine Insolvenz der L-BANK kann nicht eintreten, so dass eine Abdeckung der finanziellen Verantwortung durch Versicherungen nicht erforderlich ist.

9.2.1 Deckungsvorsorge

Eine Insolvenz der L-BANK kann nicht eintreten, so dass eine Abdeckung der finanziellen Verantwortung durch Versicherungen nicht erforderlich ist.

9.2.2 Weitere Vermögenswerte

Eine Insolvenz der L-BANK kann nicht eintreten, so dass eine Abdeckung der finanziellen Verantwortung durch Versicherungen nicht erforderlich ist.

9.2.3 Versicherung oder Garantie für Zertifikatsinhaber

Ein Versicherungsschutz für Zertifikatsinhaber ist nicht gegeben.

9.3 Vertraulichkeit von Geschäftsinformationen

9.3.1 Vertraulich zu behandelnde Daten

Alle Informationen und Daten über Zertifikatsinhaber und Teilnehmer der L-BANK-PKI, die nicht unter Ziffer 9.3.2 fallen, werden als vertrauliche Informationen eingestuft.

9.3.2 Nicht vertraulich zu behandelnde Daten

Alle Informationen und Daten, die in herausgegebenen Zertifikaten und Sperrlisten explizit (z. B. E-Mail-Adresse) oder implizit (z. B. Daten über die Zertifizierung) enthalten sind oder davon abgeleitet werden können, werden als nicht vertraulich eingestuft.

9.3.3 Verantwortung zum Schutz vertraulicher Informationen

Die L-BANK-PKI trägt die Verantwortung für Maßnahmen zum Schutz vertraulicher Informationen.

9.4 Schutz personenbezogener Daten

9.4.1 Richtlinie zur Verarbeitung personenbezogener Daten

Die Speicherung und Verarbeitung von personenbezogenen Daten richtet sich nach den gesetzlichen Datenschutzbestimmungen.

9.4.2 Vertraulich zu behandelnde Daten

Jegliche Daten über Zertifikatsinhaber und Teilnehmer der L-BANK-PKI werden vertraulich behandelt.

9.4.3 Nicht vertraulich zu behandelnde Daten

Es gelten die Bestimmungen in Abschnitt 9.3.2.

9.4.4 Verantwortung zum Schutz personenbezogener Daten

Die L-BANK-PKI trägt die Verantwortung für Maßnahmen zum Schutz personenbezogener Daten.

9.4.5 Einwilligung und Nutzung personenbezogener Daten

Der Zertifikatsinhaber stimmt der Nutzung von personenbezogenen Daten durch die L-BANK-PKI zu, soweit dies zur Leistungserbringung erforderlich ist. Darüber hinaus können alle Informationen veröffentlicht werden, die als nicht vertraulich behandelt werden.

9.4.6 Offenlegung bei gerichtlicher Anordnung oder im Rahmen gerichtlicher Beweisführung

Die L-BANK-PKI richtet sich bei der Speicherung und Verarbeitung von personenbezogenen Daten nach den gesetzlichen Datenschutzbestimmungen. Eine Offenlegung findet gegenüber staatlichen Instanzen nur bei Vorliegen entsprechender Entscheidungen in Übereinstimmung mit den geltenden Gesetzen statt.

9.4.7 Andere Umstände einer Veröffentlichung

Es sind keine weiteren Umstände für eine Veröffentlichung vorgesehen.

9.5 Urheberrechte

Die L-BANK ist Urheber dieses Dokumentes. Das Dokument kann unverändert an Dritte weitergegeben werden.

9.6 Verpflichtungen

9.6.1 Verpflichtung der Zertifizierungsstellen

Die L-BANK-PKI verpflichtet sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

9.6.2 Verpflichtung der Registrierungsstellen

Die L-BANK-PKI sowie die in die Registrierung eingebundenen Stellen verpflichten sich, den Bestimmungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) zu folgen.

9.6.3 Verpflichtung des Zertifikatsinhabers

Die Verpflichtung des Zertifikatsinhabers ist in Abschnitt 4.5.1 geregelt.

9.6.4 Verpflichtung der Zertifikatsnutzers

Die Verpflichtung des Zertifikatsnutzers ist in Abschnitt 4.5.2 geregelt. Darüber hinaus muss er den Zertifikatsrichtlinien seiner Organisation folgen.

9.6.5 Verpflichtung anderer Teilnehmer

Von der L-BANK-PKI beauftragte Dienstleister (z. B. Betreiber von Verzeichnisdiensten) werden auf die Einhaltung dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) verpflichtet.

9.7 Gewährleistung

Grundsätzlich wird keine Gewährleistung übernommen. Die L-BANK garantiert nicht die Verfügbarkeit der Leistungen der PKI.

9.8 Haftungsbeschränkung

Verletzt die L-BANK bei der Vertragsdurchführung schuldhaft eine vertragswesentliche Pflicht, die hierfür im Einzelfall von besonderer Bedeutung ist, so haftet sie für den dadurch entstehenden Schaden. Bei einfacher Fahrlässigkeit ist die Haftung der L-BANK auf den vertragstypischen Schaden beschränkt.
Für die Verletzung sonstiger Pflichten haftet die L-BANK nur bei grobem Verschulden. Gegenüber Kaufleuten und öffentlichen Verwaltungen gilt die Haftungsbeschränkung des Absatz 1 Satz 2 auch bei grober Fahrlässigkeit einfacher Erfüllungsgehilfen.
Vorstehende Haftungsausschlüsse und -begrenzungen finden keine Anwendung auf die Haftung für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit; insofern haftet die L-BANK nach den gesetzlichen Bestimmungen.

Im Falle einer Haftung der L-BANK nach den vorstehenden Absätzen bestimmt sich der Haftungsumfang entsprechend § 254 BGB danach, wie das Verschulden der L-BANK im Verhältnis zu anderen Ursachen an der Entstehung des Schadens mitgewirkt hat.

9.9 Haftungsfreistellung

Bei der unsachgemäßen Verwendung des Zertifikats und dem zugehörigen privaten Schlüssel oder einer Verwendung des Schlüsselmaterials beruhend auf fälschlichen oder fehlerhaften Angaben bei der Beantragung ist die L-BANK von der Haftung freigestellt.

9.10 Inkrafttreten und Aufhebung

9.10.1 Inkrafttreten

Diese Zertifizierungsrichtlinie (CP) und die Regelungen für den Zertifizierungsbetrieb (CPS) treten an dem Tag in Kraft, an dem sie gemäß Kapitel 2 veröffentlicht werden.

9.10.2 Aufhebung

Dieses Dokument ist so lange gültig, bis es durch eine neue Version ersetzt wird oder der Betrieb der L-BANK-PKI eingestellt wird.

9.10.3 Konsequenzen der Aufhebung

Von den Konsequenzen der Aufhebung dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) bleibt die Verantwortung zum Schutz vertraulicher Informationen und personenbezogener Daten unberührt.

9.11 Individuelle Benachrichtigungen und Kommunikation mit Teilnehmern

In dieser Zertifizierungsrichtlinie werden keine entsprechenden Regelungen getroffen.

9.12 Änderungen der Richtlinie

9.12.1 Vorgehen bei Änderungen

Änderungen der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) werden rechtzeitig vor ihrem Inkrafttreten veröffentlicht.

9.12.2 Benachrichtigungsmechanismus und Fristen

Die Zertifikatsinhaber werden rechtzeitig vor dem Inkrafttreten auf die Änderung der Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) per signierter E-Mail hingewiesen.

Das Einverständnis von Geschäftspartnern mit den Änderungen gilt als erteilt, wenn der L-BANK-PKI bis zum Zeitpunkt des Inkrafttretens keine gegenteilige Erklärung mit signierter E-Mail zugeht. Auf diese Folge wird die L-BANK-PKI bei dem Hinweis auf die Änderung besonders aufmerksam machen.
Beschäftigten der L-BANK gegenüber gilt die im Intranet bekannt gemachte jeweils aktuelle Fassung.

9.12.3 Umstände, die eine Änderung des Richtlinienbezeichners (OID) erfordern

Der Richtlinienbezeichner ändert sich bis zum Ende der Gültigkeit der zugehörigen Zertifizierungsinstanz nicht.

9.13 Schiedsverfahren

Die Anrufung eines Schiedsverfahrens liegt im Ermessen der L-BANK.

9.14 Gerichtsstand

Der Gerichtsstand ist Karlsruhe.

9.15 Konformität mit geltendem Recht

Es gilt deutsches Recht. Die von der L-BANK-PKI ausgestellten Zertifikate sind nicht konform zu qualifizierten Zertifikaten gemäß Signaturgesetz.

9.16 Weitere Regelungen

9.16.1 Vollständigkeit

Alle Regelungen in dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS) gelten zwischen der L-BANK-PKI und den Zertifikatsinhabern. Die Ausgabe einer neuen Version ersetzt alle vorherigen Versionen. Mündliche Vereinbarungen bzw. Nebenabreden sind nicht zulässig.

9.16.2 Abtretung der Rechte

Eine Abtretung von Rechten ist nicht vorgesehen.

9.16.3 Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Zertifizierungsrichtlinie unwirksam sein oder werden, so lässt dies den übrigen Inhalt der Zertifizierungsrichtlinie unberührt. Auch eine Lücke berührt nicht die Wirksamkeit der Zertifizierungsrichtlinie im Übrigen. Anstelle der unwirksamen Bestimmung gilt diejenige wirksame Bestimmung als vereinbart, welche der ursprünglich gewollten am nächsten kommt oder nach Sinn und Zweck der Zertifizierungsrichtlinie geregelt worden wäre, sofern der Punkt bedacht worden wäre.

9.16.4 Rechtliche Auseinandersetzungen / Erfüllungsort

Rechtliche Auseinandersetzungen, die aus dem Betrieb der L-BANK-PKI herrühren, obliegen den Gesetzen der Bundesrepublik Deutschland.

Erfüllungsort und Gerichtsstand ist Karlsruhe.

9.16.5 Force Majeure

Die L-BANK übernimmt keine Haftung für die Verletzung einer Pflicht sowie für Verzug oder Nichterfüllung im Rahmen dieser Zertifizierungsrichtlinie (CP) und den Regelungen für den Zertifizierungsbetrieb (CPS), sofern das zugrunde liegende Ereignis außerhalb ihrer Kontrolle (z. B. höhere Gewalt, Kriegshandlungen, Netzausfälle, Brände, Erdbeben und andere Katastrophen) resultiert.

9.17 Andere Regelungen

Entfällt.

10 Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnologie
C	Country (Bestandteil des Distinguished Name)
CA	Certification Authority, Zertifizierungsinstanz
CN	Common Name (Bestandteil des Distinguished Name)
CP	Certificate Policy; Zertifizierungsrichtlinie einer PKI
CPS	Certification Practice Statement, Regelungen für den Zertifizierungsbetrieb
CRL	Certificate Revocation List, Sperrliste
CRLDP	Sperrlistenverteilpunkt
DN	Distinguished Name
DName	Distinguished Name
EMAIL	Email address (Bestandteil des Distinguished Name)
EBCA	European Bridge CA, Verknüpfung von Public-Key-Infrastrukturen einzelner Organisationen
EMS	E-Mailsicherheit
Hardwaretoken	Hardware zur Speicherung von privaten Schlüsseln
HSM	Hardware Security Module
LDAP	Light Directory Access Protocol, Verzeichnisdienst
O	Organization (Bestandteil des Distinguished Name)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit (Bestandteil des Distinguished Name)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PSE	Personal Secure Environment
RA	Registration Authority, Registrierungsstelle
RFC	Request for Comment, Dokumente für weltweite Standardisierungen
RFC3647	Dieser RFC dient der Beschreibung von Dokumenten, die den Betrieb einer PKI beschreiben
RFC822 Name	E-Mail Adresse
Root-CA	oberste Zertifizierungsinstanz einer PKI
RSA	Rivest, Shamir, Adleman
SHA-1	Secure Hash Algorithm No. 1
SigG	Signaturgesetz - Gesetz über Rahmenbedingungen für elektronische Signaturen
S/MIME	Secure Multipurpose Internet Mail Extensions, Standard für sichere E-Mail
Sperrliste	signierte Liste einer CA, die gesperrte Zertifikate enthält
SSL	Secure Socket Layer, Protokoll zur Transportsicherung einer Client-Server-Kommunikation
SÜG	Sicherheitsüberprüfungsgesetz
X.500	Protokolle und Dienste für ISO konforme Verzeichnisse
X.509v1	Zertifizierungsstandard
Zertifikat	sichere Zuordnung von öffentlichen Schlüsseln zu einem Teilnehmer

11 Informationen zum Dokument

Siehe Abschnitt 1.2.